Exhibit R-2, RDT&E Budget Item Justification: PB 2021 Navy											Date: February 2020	
Appropriation/Budget Activity 1319: *Research, Development, Test & Evaluation, Navy I* BA 7: *Operational Systems Development*					R-1 Program Element (Number/Name) PE 0303140N *I Information Sys Security Program*							
COST ($ in Millions)	**Prior Years**	**FY 2019**	**FY 2020**	**FY 2021 Base**	**FY 2021 OCO**	**FY 2021 Total**	**FY 2022**	**FY 2023**	**FY 2024**	**FY 2025**	**Cost To Complete**	**Total Cost**
Total Program Element	504.615	43.348	44.853	39.094	-	39.094	33.888	34.136	34.889	35.209	Continuing	Continuing
0734: *Communications Security R&D*	484.190	41.083	39.713	36.924	-	36.924	31.672	31.880	32.588	32.862	Continuing	Continuing
3230: *Information Assurance*	20.425	2.265	2.140	2.170	-	2.170	2.216	2.256	2.301	2.347	Continuing	Continuing
9999: *Congressional Adds*	0.000	0.000	3.000	0.000	-	0.000	0.000	0.000	0.000	0.000	0.000	3.000

A. Mission Description and Budget Item Justification

The Information Systems Security Program (ISSP) ensures the protection of Navy and Navy hosted joint telecommunication and Information Technology (IT) systems from cyber exploitation and attack. The ISSP extends cybersecurity to ensure confidentiality, integrity, and availability of these systems and content processed, stored, or transmitted therein by performing the acquisition, modernization and sustainment of cybersecurity platforms and systems; cyberspace operations include both defensive and offensive measures, which preserve the ability to protect data, networks, net-centric capabilities, and other designated systems while projecting power by the application of force in or through cyberspace. The ISSP includes the protection of the Navy's National Security Systems (NSS). The ISSP must be rapid, predictive, adaptive, and tightly coupled to cyberspace technology. The ISSP provides cybersecurity systems and infrastructure based on mission impacts, cybersecurity threats, information criticality, vulnerabilities, and required defensive countermeasure capabilities.

The ISSP focuses on efforts that address the risk management of cyberspace, which provides capabilities to protect, detect, restore and respond. The ISSP provides the Navy with the following cybersecurity elements: (1) defense of NSS, including the Nuclear Command, Control, and Communications, Navy (NC3-N) system, naval weapons systems, critical naval infrastructure for Command, Control, Communications, Computers, & Intelligence (C4I) afloat and shore networks, joint time and navigation systems, and industrial control systems, using modern cryptographic solutions and cyber security tools; (2) technologies for the Navy's Computer Network Defense (CND) service provider that accelerates the Navy's ability to prevent, constrain, and mitigate cyber attacks and critical vulnerabilities; (3) Navy Cyber Situational Awareness (NCSA) technologies that provides the operational context for cyber threat intelligence and Situational Awareness (SA), from external boundaries to tactical edge infrastructures; (4) assurance of the Navy's Cryptography (Crypto) telecommunications infrastructure and the wireless spectrum; (5) sensing cyber threats across all Navy shore and afloat networks to expand the capabilities of monitoring, assessing, and detecting adversary activities across multiple enclaves through the collection of tools in SHARKCAGE; (6) assurance of joint-user cyberspace domains, using a Defense-In-Depth (DiD) security architecture and its alignment with the Joint Information Environment (JIE)/Joint Regional Security Stack (JRSS); (7) assurance technologies, including Key Management (KM) and Public Key Infrastructure (PKI).

Exhibit R-2, RDT&E Budget Item Justification: PB 2021 Navy	Date: February 2020
Appropriation/Budget Activity 1319: *Research, Development, Test & Evaluation, Navy I* BA 7: *Operational Systems Development*	**R-1 Program Element (Number/Name)** PE 0303140N *I Information Sys Security Program*

B. Program Change Summary ($ in Millions)	FY 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total
Previous President's Budget	44.228	41.853	38.841	-	38.841
Current President's Budget	43.348	44.853	39.094	-	39.094
Total Adjustments	-0.880	3.000	0.253	-	0.253
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	3.000			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-0.002	0.000			
• SBIR/STTR Transfer	-0.877	0.000			
• Program Adjustments	0.000	0.000	0.331	-	0.331
• Rate/Misc Adjustments	-0.001	0.000	-0.078	-	-0.078

Congressional Add Details ($ in Millions, and Includes General Reductions)	FY 2019	FY 2020
Project: 9999: *Congressional Adds*		
Congressional Add: *High assurance infrastructure in defense systems*	0.000	3.000
Congressional Add Subtotals for Project: 9999	0.000	3.000
Congressional Add Totals for all Projects	0.000	3.000

Change Summary Explanation

TECHNICAL:

Key Management (KM):
- Capability Increment (CI)-2 Spiral 2 Full Deployment Decision (FDD) renamed to CI-2 Maintenance Revision (MR)-2 Milestone FDD.

SCHEDULE:

Computer Network Defense (CND):
- Starting in FY21, schedule updated to reflect CND Inc 2's migration from specific "capability builds" to a continuous capability enhancement strategy. This strategy specifically addresses end of life and end of support components. The Cybersecurity tools fielded in the Fleet are commercial off-the-shelf (COTS) products that are regularly improved with the latest technologies. CND designs, integrates, tests, and fields these products to protect the Navy's tactical networks from the evolving cyber threat.

Exhibit R-2, RDT&E Budget Item Justification: PB 2021 Navy	Date: February 2020
Appropriation/Budget Activity 1319: *Research, Development, Test & Evaluation, Navy I* BA 7: *Operational Systems Development*	**R-1 Program Element (Number/Name)** PE 0303140N *I Information Sys Security Program*

Navy Cryptography (Crypto):
- All KGV-11M milestones shifted due to change in developmental contract award schedule; no impact to programmatic schedule.
Advanced Cryptographic Capability (ACC) schedule updates are a result of a change in NSA software release date.
- Added ACC NSA Software Certification to Q3FY19.

Key Management (KM):
- CI-3 Spiral 3 Spin 1 Milestone Full Rate Production Decision (FRPD)/Fielding Decision (FD) shifted from Q3FY21 to Q1FY23 in accordance with NSA schedule.
- CI-3 Spiral 3 Spin 2 Development, Integration and Test start shifted from Q1FY20 to Q1FY21 in accordance with NSA schedule.
- Key Management Infrastructure (KMI) Tech Refresh initial delivery shifted from Q3FY20 to Q1FY21 in accordance with NSA schedule.

SHARKCAGE
- Rapid Deployment Capability (RDC) and related milestone completion shifted from Q2FY19 to Q3FY19 to allow for the development of additional capabilities per the RDC Continuation Acquisition Decision Memorandum.

Navy Cyber Situational Awareness (NCSA)
- Rapid Deployment Capability (RDC) completion and related milestones shifted from Q2FY19 to Q1FY20 due to additional required software updates per the RDC Continuation Acquisition Decision Memorandum Developmental Testing results.
- Limited Deployment Decision shifted from Q3FY19 to Q1FY20 in accordance with RDC milestones.

FUNDING:

Computer Network Defense (CND) (+$1.502M)
- FY21 increase is due to Vulnerability Remediation Asset Manager (VRAM) 3.0 development efforts to replace VRAM 2.0 end-of-life, and development work to optimize VRAM for the cloud environment.

Navy Cryptography (Crypto)(-$3.553M):
- FY21 decrease is due to the completion of the development efforts of KGV-11M End Cryptographic Units (ECU).

Key Management (KM) (+$0.214M):
- FY21 increase aligns to the initial development of CI-3 Spiral 3 Spin 2 Development, Integration and Testing.

Navy Cyber Situational Awareness (NCSA) (-$1.005M):

Exhibit R-2, RDT&E Budget Item Justification: PB 2021 Navy	Date: February 2020
Appropriation/Budget Activity 1319: *Research, Development, Test & Evaluation, Navy I* BA 7: *Operational Systems Development*	**R-1 Program Element (Number/Name)** PE 0303140N *I Information Sys Security Program*

- FY21 decrease reflects a realignment within NCSA from Research, Development, Test and Evaluation (RDT&E) to Operations and Maintenance, Navy (OM,N) due to a change in engineering and fielding strategy to be a predominantly software solution hosted by other planned Defensive Cyberspace Operations/ Network Operations (DCO/NETOPS) systems.

Exhibit R-2A, RDT&E Project Justification: PB 2021 Navy											Date: February 2020	
Appropriation/Budget Activity 1319 / 7					R-1 Program Element (Number/Name) PE 0303140N / *Information Sys Security Program*				Project (Number/Name) 0734 / *Communications Security R&D*			
COST ($ in Millions)	**Prior Years**	**FY 2019**	**FY 2020**	**FY 2021 Base**	**FY 2021 OCO**	**FY 2021 Total**	**FY 2022**	**FY 2023**	**FY 2024**	**FY 2025**	**Cost To Complete**	**Total Cost**
0734: *Communications Security R&D*	484.190	41.083	39.713	36.924	-	36.924	31.672	31.880	32.588	32.862	Continuing	Continuing
Quantity of RDT&E Articles		-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

The Information Systems Security Program (ISSP) Research Development Test & Evaluation (RDT&E) efforts extend our cybersecurity and resiliency, provide Defensive Cyberspace Operations (DCO), and cross domain solutions to protect data, Department of Defense (DoD) Information Networks (DoDIN), net-centric operations, the forward deployed, and other designated systems in order to protect cyberspace and critical warfighting capabilities.

This project includes a rapidly evolving development, design and application integration effort to modernize cryptographic equipment and ancillaries with state-of-the-art replacements to counter evolving and increasingly sophisticated threats. Communications Security (COMSEC) and Transmission Security (TRANSEC) are evolving from stand-alone, dedicated devices to embedded modules incorporating National Security Agency (NSA) approved cryptographic engines, loaded with the certified algorithms and keys, and interconnected via industry-defined interfaces. This includes the DoDIN capability requirements document for the development of Content Based Encryption (CBE).

Computer Network Defense (CND): The CND program provides cyberspace capabilities to secure the Cyber Domain. CND is a combination of hardware, software, sets of processes and protective measures that use computer networks to detect, monitor, protect, analyze and defend against network infiltrations resulting in service/network denial, degradation and disruptions. CND enables a government or military institute/organization to defend against network attacks perpetrated by malicious or adversarial computer systems or networks.

Navy Cryptography (Crypto): Navy Crypto modernizes legacy cryptographic equipment which includes families of COMSEC and TRANSEC devices that are divided into crypto voice, crypto data, crypto products and associated ancillary devices. These devices provide modern cryptographic solutions to replace obsolete, legacy devices within the crypto categories.

Key Management (KM): KM monitors and tracks capability verification testing, designs and tests capabilities to provide a net-centric web based architecture, for the ordering, management, and distribution of all cryptographic key material to support Navy users, to include integration of Intermediary Application (iApp).

Public Key Infrastructure (PKI): The DoD PKI program, under the authority of the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD AT&L), develops and tests PKI equipment and is responsible for meeting statutory and regulatory requirements for the DoD PKI program. The Navy PKI program tests and implements products for afloat networks and shore non-Navy Marine Corps Intranet (NMCI) networks and institutionalizes Identity, Credential and Access Management (ICAM) so that person and non-person entities can securely access all authorized DoD resources.

Exhibit R-2A, RDT&E Project Justification: PB 2021 Navy		Date: February 2020
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 0734 / *Communications Security R&D*

SHARKCAGE: SHARKCAGE is a global, federated Defensive Cyberspace Operations (DCO) enclave consisting of shore sensor nodes, DCO analysis workbenches, and analytic suites. Utilizing one-way passive taps in a protected, isolated, classified environment, SHARKCAGE consolidates cyber event data from multiple platforms and networks, providing Navy DCO forces with a shared environment and common platform for integrated workflow, collaboration, and analysis. SHARKCAGE efficiently detects, correlates, and analyzes nation and non-nation state attacks against maritime Navy networks and the Naval Networking Environment (NNE).

Navy Cyber Situational Awareness (NCSA): NCSA is a command and control infrastructure that provides Navy commanders with timely, trusted, and comprehensive Situational Awareness (SA) of the cyberspace domain to include tailored, near real-time visualization of network health, vulnerabilities, and operational readiness through the correlation of data from multiple sources. NCSA combines asset data, baseline configuration data, and real-time threat data which is critical for defending a fully-interconnected network infrastructure. NCSA enables early threat detection and timely decision making.

Cybersecurity Services: Cybersecurity Services develops cyber architecture and provides cybersecurity engineering for the DoD and Department of the Navy (DoN) cybersecurity interests based on the requirements prioritized by Fleet Cyber Command/Commander Tenth Fleet (FCC/C10F). Cybersecurity Services transitions new technologies to address current Navy cybersecurity challenges.

FY21 will focus on efforts that address the risk management of cyberspace, which provides capabilities to identify, protect, detect, restore and respond. The ISSP provides the Navy with the following cybersecurity elements: (1) defense of National Security Systems (NSS), including the Nuclear Command, Control, and Communications, Navy (NC3-N) system, naval weapons systems, critical naval infrastructure for Command, Control, Communications, Computers, & Intelligence (C4I) afloat and shore networks, joint time and navigation systems, and industrial control systems, using modern cryptographic solutions and cyber security tools; (2) technologies supporting the Navy's Computer Network Defense (CND) service provider that will help the Navy's ability to prevent, constrain, and mitigate cyber attacks and critical vulnerabilities; (3) Navy Cyber Situational Awareness (NCSA) technologies that provides the operational context for cyber threat intelligence and Situational Awareness (SA), from external boundaries to tactical edge infrastructures; (4) assurance of the Navy's Crypto telecommunications infrastructure and the wireless spectrum; (5) sensing cyber threats across all Navy shore and afloat networks to expand the capabilities of monitoring, assessing, and detecting adversary activities across multiple enclaves through the collection of tools in SHARKCAGE;(6) assurance of joint-user cyberspace domains, using a Defense-In-Depth (DiD) security architecture and its alignment with the Joint Information Environment (JIE)/Joint Regional Security Stack (JRSS); (7) assurance technologies, including Key Management (KM) and Public Key Infrastructure (PKI).

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total
Title: Computer Network Defense (CND)	12.911	13.501	15.003	0.000	15.003
Articles:	-	-	-	-	-
FY 2020 Plans: - Due to the dynamic nature of cybersecurity and increasing complexity of technology, CND Inc 2 will continue capability enhancement Research and Development (R&D) efforts.					

Exhibit R-2A, RDT&E Project Justification: PB 2021 Navy		Date: February 2020
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 0734 / *Communications Security R&D*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total
- Continue to develop and enhance Navy's portion of the Nuclear Command, Control, and Communications, Navy (NC3-N) and Ballistic Missile Defense (BMD) cyber security system of systems within the CND architecture. - Complete Next Generation Firewall upgrades to address end of life issues, enable centralized firewall management functionality, and enhance security of the network. - Complete Virtual Training Environment (VTE) hardware and software upgrades and enhancements including remote replication and hosting of critical endpoint security management servers. - Begin cybersecurity enhancements of Vulnerability Asset Remediation Manager (VRAM) to improve Department of Defense (DoD) cyber readiness and upgrade to VRAM 3.0 with improved capabilities in response to urgent Operation Orders (OPRDs) and Tasking Orders (TASKORDs). - Begin major CND operating system upgrades, out of band management network hardware and software switching, routing and firewall upgrades and Next Generation Intrusion Prevention and Content Scanning System upgrades. - Continue to implement DoD and United States Cyber Command (USCC) cybersecurity tools and mandates into Outside Continental United States (OCONUS) Navy Enterprise Network (ONE-Net) and Command, Control, Communication, Computers, & Intelligence (C4I) networks. - Continue to provide technical guidance to support Consolidated Afloat Network and Enterprise Services (CANES) deployment of new CND capabilities. - Continue to optimize CND suite for alignment with Joint Regional Security Stack (JRSS). - Continue to develop, integrate, and test solutions to replace and assume acquisition management of Navy Cyber Defense Operations Command's (NCDOC) tactical sensor infrastructure. - Continue development and alignment to Navy's Insider Threat program to identify possible insider threats across multiple enclaves in order to fulfill the Presidential, DoD, and Department of Navy (DoN) directives.					
FY 2021 Base Plans: - FY21 increase is due to VRAM 3.0 development efforts to replace VRAM 2.0 end-of-life, and development work to optimize VRAM for the cloud environment. - Begin major CND security operation workstation upgrades, upgrades to Load Balancers, addressing endpoint security gaps in the CND Architecture and updates to the Detonation Malware Analysis Capability at NCDOC. - Complete CND operating system upgrades, out of band management and Next Generation Intrusion Prevention, and enhance security of the network. - Complete VTE hardware and software upgrades and enhancements including remote replication and hosting of critical endpoint security management servers.					

Exhibit R-2A, RDT&E Project Justification: PB 2021 Navy		Date: February 2020
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 0734 / *Communications Security R&D*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total
- Continue cybersecurity enhancements of VRAM to improve DoD cyber readiness and upgrade to VRAM 3.0 with improved capabilities in response to urgent OPRDs and TASKORDs. - Continue to develop and enhance Navy's portion of the NC3-N and BMD cyber security system of systems within the CND architecture. - Continue to implement DoD and USCC cybersecurity tools and mandates into ONE-Net and C4I networks. - Continue to provide technical guidance to support CANES deployment of new CND capabilities. - Continue to optimize CND suite for alignment with JRSS. - Continue efforts to further virtualize CND capabilities for more effective and cost-efficient deployment of cybersecurity technologies. - Continue to develop, integrate, and test solution to replace and assume acquisition management of NCDOC tactical sensor infrastructure. ***FY 2021 OCO Plans:*** N/A ***FY 2020 to FY 2021 Increase/Decrease Statement:*** FY21 increase is due to Vulnerability Asset Remediation Manager (VRAM) 3.0 development efforts to replace VRAM 2.0 end-of-life, and development work to optimize VRAM for the cloud environment.					
Title: Navy Cryptography (Crypto)	13.258	10.827	7.274	0.000	7.274
Articles:	-	-	-	-	-
FY 2020 Plans: - Continue development of Advanced Cryptographic Capabilities (ACC) security software of various Communications Security (COMSEC) devices and compatibility of cryptographic devices capable of receiving software updates. - Continue developing a transition plan for Transmission Security (TRANSEC) and ACC for crypto modernization. - Continue KGV-11M product development and continue developmental testing. - Complete KGV-11M Developmental Test & Evaluation (DT&E). - Continue to provide development and security engineering for modernization of Department of Navy (DoN) crypto systems and embeddable crypto modernization strategies. - Continue to work with National Security Agency (NSA) on certification authority and data testing for all crypto modernization efforts. - Continue to investigate impacts of upcoming NSA security enhancements for crypto modernization products.					

Exhibit R-2A, RDT&E Project Justification: PB 2021 Navy		Date: February 2020
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 0734 / *Communications Security R&D*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total
- Continue to enhance and modernize VINSON/Advanced Narrowband Digital Voice Terminal (ANDVT) Cryptographic Modernization (VACM) ancillary devices. - Continue to develop Navy strategy and implementation plan to modernize secure voice architectures within Navy networks. ***FY 2021 Base Plans:*** -FY21 decrease is due to the completion of a three-year development effort of KGV-11M End Cryptographic Units (ECU). - Complete KGV-11M NSA Certification to initiate the Full Rate Production (FRP) for KGV-11M. - Continue to provide development and security engineering for modernization of DoN crypto systems and embeddable crypto modernization strategies. - Continue to work with NSA on certification authority and data testing for all crypto modernization efforts. - Continue to investigate impacts of upcoming NSA security enhancements for crypto modernization products. - Continue to enhance and modernize VACM ancillary devices. - Continue to develop Navy strategy and implementation plan to modernize secure voice architectures within Navy networks. ***FY 2021 OCO Plans:*** N/A ***FY 2020 to FY 2021 Increase/Decrease Statement:*** -FY21 decrease is due to the completion of a three-year development effort of KGV-11M End Cryptographic Units (ECU).					
Title: Key Management (KM)	0.823	0.802	1.016	0.000	1.016
Articles:	-	-	-	-	-
FY 2020 Plans: - Continue migrating Communications Security (COMSEC) Management Workstation (CMWS) and the follow on to Simple Key Loader (SKL) into the Key Management Infrastructure (KMI) environment. - Continue the development, engineering and testing of KMI Capability Increment (CI)-3, Spiral 3 Spin 1 including the integration of Intermediary Application (iApp) within a network environment, which will enhance the accounting for and distribution of KMI key delivery. - Complete the development, engineering and testing of KMI Tech Refresh. ***FY 2021 Base Plans:***					

Exhibit R-2A, RDT&E Project Justification: PB 2021 Navy		Date: February 2020
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 0734 / *Communications Security R&D*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total
- FY21 increase aligns to the initial development of CI-3 Spiral 3 Spin 2 Development, Integration and Testing. - Begin the development, engineering and testing of KMI CI-3, Spiral 3 Spin 2. - Continue migrating COMSEC CMWS and the follow on to SKL into the KMI environment. - Complete the development, engineering and testing of KMI CI-3, Spiral 3 Spin 1 including the integration of iApp within a network environment, which will enhance the accounting for and distribution of KMI key delivery. ***FY 2021 OCO Plans:*** N/A ***FY 2020 to FY 2021 Increase/Decrease Statement:*** FY21 increase aligns to the initial development of CI-3 Spiral 3 Spin 2 Development, Integration and Testing.					
Title: Public Key Infrastructure (PKI)	0.366	0.373	0.405	0.000	0.405
Articles:	-	-	-	-	-
FY 2020 Plans: - Continue Navy compliance and compatibility with Department of Defense (DoD) PKI implementation, cryptographic algorithms and development efforts, to include Computer Network Defense (CND), enhanced algorithms and other encryption methodologies, Navy Certificate Validation Infrastructure (NCVI), enhancements for afloat and shore environments, Common Access Card (CAC) configuration modifications, Network (NIPRNet) Enterprise Alternate Token System (NEATS), Non-Person Entity (NPE), and Secret Internet Protocol Router Network (SIPRNET) Token Management System. ***FY 2021 Base Plans:*** - Continue Navy compliance and compatibility with DoD PKI implementation, cryptographic algorithms and development efforts, to include CND, enhanced algorithms and other encryption methodologies, NCVI enhancements for afloat and shore environments, CAC configuration modifications, NEATS, NPE, and SIPRNet Token Management System. ***FY 2021 OCO Plans:*** N/A ***FY 2020 to FY 2021 Increase/Decrease Statement:*** No significant changes from FY20 to FY21.					
Title: SHARKCAGE	5.202	6.796	6.754	0.000	6.754
Articles:	-	-	-	-	-

Exhibit R-2A, RDT&E Project Justification: PB 2021 Navy		Date: February 2020
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 0734 / *Communications Security R&D*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total
FY 2020 Plans: - Continue development efforts to incorporate Nuclear Command, Control, and Communications, Navy (NC3-N) missions within the SHARKCAGE environment (details held at a higher classification). - Continue development of SHARKCAGE Defensive Cyberspace Operations (DCO) enclave to address requirements from the fleet in light of emerging threats in the tactical environment. Development efforts include network taps, sensors, and analytic toolsets for passively monitoring multiple Navy shore and afloat networks and enclaves (e.g., Command, Control, Communications, Computers and Intelligence (C4I) networks, Combat Systems (CS), Hull, Mechanical, and Electrical (HM&E), etc.) to detect and assess cyber threats across multiple security enclaves. - Continue development of event collection and analysis components for shore sensor nodes and afloat flyaway kits for deployed Cyber Protection Teams (CPT). ***FY 2021 Base Plans:*** - Begin development, engineering and testing of replacement hardware for end of life/sale components fielded at initial installation sites. - Continue to xpand the NC3-N mission's capability within the SHARKCAGE environment (details held at a higher classification). - Continue to enhance capabilities to the SHARKCAGE DCO enclave to address additional fleet requirements as the emerging threats evolve. Development efforts include network taps, sensors, and analytic toolsets for passively monitoring multiple Navy shore and afloat networks and enclaves. - Continue to expand the development of analysis components and event collection activities for shore nodes and afloat units for the deployed CPT community. ***FY 2021 OCO Plans:*** N/A ***FY 2020 to FY 2021 Increase/Decrease Statement:*** No significant changes from FY20 to FY21.					
Title: Navy Cyber Situational Awareness (NCSA)	6.214	5.025	4.020	0.000	4.020
Articles:	-	-	-	-	-
FY 2020 Plans: - Continue the integration of all-source intelligence with Navy maritime data to enable early threat detection, and assessment of adversary activities and capabilities, intent, and access to critical Navy networks.					

Exhibit R-2A, RDT&E Project Justification: PB 2021 Navy		Date: February 2020
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 0734 / *Communications Security R&D*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total
- Continue the development of a shared and tailorable Maritime Cyber "Integrated" Common Operational Picture (COP) external to Fleet Cyber Command/Commander Tenth Fleet (FCC/C10F) to include all geographic Maritime Operations Centers (MOCs) to enable assessments of cyber vulnerabilities, threats, and risks relative to Navy missions. - NCSA maturation will continue to provide monitoring of relevant and current Navy networks providing near real-time visualization and analytics of the cyberspace domain. ***FY 2021 Base Plans:*** - FY21 decrease reflects a realignment within NCSA from Research, Development, Test and Evaluation (RDT&E) to Operations and Maintenance, Navy (OM,N) due to a change in engineering and fielding strategy to be a predominantly software solution hosted by other planned Defensive Cyberspace Operations/ Network Operations (DCO/NETOPS) systems. - Shift engineering strategy to be a predominantly software solution providing monitoring of relevant Navy networks providing near real-time visualization and analytics of the cyberspace domain in Navy mission context. - Continue the development of a shared and tailorable Maritime Cyber "Integrated" COP external to FCC/C10F to include all geographic MOCs to enable assessments of cyber vulnerabilities, threats, and risks relative to Navy missions. - NCSA maturation will provide monitoring of relevant and current Navy networks providing near real-time visualization and analytics of the cyberspace domain. ***FY 2021 OCO Plans:*** N/A ***FY 2020 to FY 2021 Increase/Decrease Statement:*** - FY21 decrease reflects a realignment within NCSA from Research, Development, Test and Evaluation (RDT&E) to Operations and Maintenance, Navy (OM,N) due to a change in engineering and fielding strategy to be a predominantly software solution hosted by other planned Defensive Cyberspace Operations/ Network Operations (DCO/NETOPS) systems.					
Title: Cybersecurity Services	2.309	2.389	2.452	0.000	2.452
Articles:	-	-	-	-	-
FY 2020 Plans: - Continue coordination and alignment with Joint Information Environment (JIE) (e.g., Joint Regional Security Stack (JRSS), Joint Management System (JMS), Tactical Processing Node (TPN) etc.) to ensure Navy architecture requirements for tactical networks are met.					

Exhibit R-2A, RDT&E Project Justification: PB 2021 Navy		Date: February 2020
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 0734 / *Communications Security R&D*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total
- Continue to provide security systems engineering support for the development of Department of Defense (DoD) and Department of Navy (DoN) cybersecurity architectures and the transition of new technologies to address Navy cybersecurity challenges. Continue to provide updates to reflect emerging priorities and address Navy specific threats. - Continue to coordinate cybersecurity activities across the virtual System Command (SYSCOM) via the Cybersecurity Trusted Architecture (TA) to ensure the security design and integration of cybersecurity products and services is consistent across the Navy for major initiatives such as the future afloat, ashore, and Outside of the Continental United States (OCONUS) networks. - Continue to provide cybersecurity risk analysis and recommended risk mitigation strategies for Navy critical networks and Command, Control, Communication, Computers, & Intelligence (C4I) systems. Continue to coordinate with the Navy acquisition community to ensure cybersecurity requirements are identified and addressed within the development cycles for emerging Navy network and C4I capabilities. - Continue to evaluate products for security issues and develop guidance and procedures for the design and integration of risk mitigation strategies via appropriate cybersecurity controls.					
FY 2021 Base Plans: - Continue coordination and alignment with JIE (e.g., JRSS, JMS, Tactical Processing Node (TPN) etc.) to ensure Navy architecture requirements for tactical networks are met. - Continue to provide security systems engineering support for the development of DoD and DoN cybersecurity architectures and the transition of new technologies to address Navy cybersecurity challenges. Continue to provide updates to reflect emerging priorities and address Navy specific threats. - Continue to coordinate cybersecurity activities across the virtual SYSCOM via the Cybersecurity TA to ensure the security design and integration of cybersecurity products and services is consistent across the Navy for major initiatives such as the future afloat, ashore, and OCONUS networks. - Continue to provide cybersecurity risk analysis and recommended risk mitigation strategies for Navy critical networks and C4I systems. Continue to coordinate with the Navy acquisition community to ensure cybersecurity requirements are identified and addressed within the development cycles for emerging Navy network and C4I capabilities. - Continue to evaluate products for security issues and develop guidance and procedures for the design and integration of risk mitigation strategies via appropriate cybersecurity controls.					
FY 2021 OCO Plans:					

Exhibit R-2A, RDT&E Project Justification: PB 2021 Navy		Date: February 2020
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 0734 / *Communications Security R&D*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total
N/A ***FY 2020 to FY 2021 Increase/Decrease Statement:*** No significant changes from FY20 to FY21.					
Accomplishments/Planned Programs Subtotals	41.083	39.713	36.924	0.000	36.924

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total	FY 2022	FY 2023	FY 2024	FY 2025	Cost To Complete	Total Cost
• OPN/3415: *Info Systems Security Program (ISSP)*	150.099	166.540	157.551	-	157.551	155.801	163.645	165.820	165.329	Continuing	Continuing

Remarks

D. Acquisition Strategy

Computer Network Defense (CND): The CND Acquisition Category (ACAT) IVM program is a layered protection strategy, which militarizes Commercial Off-The-Shelf (COTS) and integrates Government Off-The-Shelf (GOTS) hardware and software products that collectively provide an effective network security infrastructure. The rapid advancement of cyber technology requires an efficient process for updating CND tools deployed to afloat and shore platforms. Recognizing the need for future CND capability improvements, the CND program implements an evolutionary acquisition strategy that continuously modernizes and refreshes end-of-life/end-of-service capabilities to ensure the latest cybersecurity tools are protecting the Navy's tactical networks.

Navy Cryptography (Crypto): Modernized crypto devices will replace legacy crypto in accordance with the mandate by Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510 as well as the National Security Agency (NSA) planned decertification, which improves the Navy's cyber defense posture. For Advanced Cryptographic Capability (ACC) the acquisition strategy will follow the NSA direction on mandated software upgrades. The KGV-11M program is being led by the Navy.

Key Management (KM): Key Management Infrastructure (KMI) is a NSA-led ACAT I program. It is the next generation Electronic Key Management System (EKMS) that provides the infrastructure for management, ordering and distribution of key material as well as directly supporting the key requirements of all Crypto modernization efforts. KMI will follow an increment/spiral development strategy. The KMI program will continue to develop alternative architecture implementations for communities within the Navy to implement the Intermediary Application (iApp) as a KM solution.

Public Key Infrastructure (PKI): Department of Defense (DoD) PKI is an ACAT I program jointly led by the NSA and the Defense Information Systems Agency (DISA). The Under Secretary of Defense for Acquisition, Technology and Logistics (USD AT&L) is the Milestone Decision Authority (MDA). The Navy PKI project supports the DoD-wide implementation of PKI products and services across Navy afloat, non-Navy Marine Corps Intranet (NMCI), Outside the Continental United States (OCONUS) networks and other excepted networks.

Exhibit R-2A, RDT&E Project Justification: PB 2021 Navy		Date: February 2020
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 0734 / *Communications Security R&D*

SHARKCAGE: SHARKCAGE will continue to integrate COTS and GOTS hardware and software products to monitor multiple Navy networks and enclaves to detect, analyze, and assess threats. SHARKCAGE will provide Navy Cyber Defense Operations Command (NCDOC), Navy Information Operations Centers (NIOC), Fleet Cyber Command/Commander Tenth Fleet (FCC/C10F), Cyber Protection Teams (CPT), and other CND deployers with a global Defensive Cyberspace Operations (DCO) enclave to monitor the Naval Networking Environment (NNE) and maritime Navy networks, including Navy shore sites and afloat platforms conducting Ballistic Missile Defense (BMD) and Nuclear Command, Control, and Communications, Navy (NC3-N) missions.

Navy Cyber Situational Awareness (NCSA): The NCSA Deliberate Acquisition Activities will continue to integrate COTS and GOTS hardware and software products to provide visualization of Navy networks and enclaves to analyze and assess mission threats. NCSA will be implemented via an evolutionary acquisition approach using an iterative, agile software enhancement process in the form of capability drops to address future cyber Situation Awareness (SA) capabilities and improvements required by fleet warfighters. These government-led agile software enhancements will be documented and managed through a requirements governance board process.

Cybersecurity Services: Cybersecurity Services is a Navy project, which develops cyber architecture and provides security engineering for the DoD and Department of the Navy (DoN) cybersecurity interests based on the requirements prioritized by FCC/C10F. Cybersecurity Services transitions new technologies to address current Navy cybersecurity challenges.

Exhibit R-3, RDT&E Project Cost Analysis: PB 2021 Navy		Date: February 2020
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 0734 / *Communications Security R&D*

Product Development ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2019 Cost	FY 2019 Award Date	FY 2020 Cost	FY 2020 Award Date	FY 2021 Base Cost	FY 2021 Base Award Date	FY 2021 OCO Cost	FY 2021 OCO Award Date	FY 2021 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Development (PY)	Various	Various : Various	190.205	0.000		0.000		0.000		-		0.000	0.000	190.205	-
Hardware Development (WR)	WR	NIWC PACIFIC : San Diego, CA	15.161	2.750	Oct 2018	2.641	Oct 2019	3.918	Oct 2020	-		3.918	Continuing	Continuing	Continuing
Hardware Development	C/CPFF	NIWC PACIFIC : San Diego, CA	4.245	0.809	Dec 2018	0.777	Dec 2019	2.802	Dec 2020	-		2.802	Continuing	Continuing	Continuing
Hardware Development (WR)	WR	NIWC ATLANTIC : Charleston, SC	5.644	0.531	Oct 2018	0.510	Oct 2019	0.630	Oct 2020	-		0.630	Continuing	Continuing	Continuing
Hardware Development	C/CPFF	NIWC ATLANTIC : Charleston, SC	2.827	0.995	Jan 2019	0.956	Jan 2020	1.112	Jan 2021	-		1.112	Continuing	Continuing	Continuing
Hardware Development	C/CPIF	Viasat : San Diego, CA	0.000	3.500	Apr 2019	3.100	Apr 2020	0.000		-		0.000	0.000	6.600	-
Software Development (WR)	WR	NIWC PACIFIC : San Diego, CA	32.549	7.744	Oct 2018	6.860	Oct 2019	6.482	Oct 2020	-		6.482	Continuing	Continuing	Continuing
Software Development	C/CPFF	NIWC PACIFIC : San Diego, CA	12.303	5.040	Dec 2018	4.840	Dec 2019	3.792	Dec 2020	-		3.792	Continuing	Continuing	Continuing
Software Development (WR)	WR	NIWC ATLANTIC : Charleston, SC	8.744	2.079	Oct 2018	1.997	Oct 2019	2.191	Oct 2020	-		2.191	Continuing	Continuing	Continuing
Software Development	C/CPFF	NIWC ATLANTIC : Charleston, SC	13.443	3.854	Jan 2019	3.701	Jan 2020	2.667	Jan 2021	-		2.667	Continuing	Continuing	Continuing
Software Development	FFRDC	MITRE : McLean, VA	4.844	1.883	Dec 2018	1.808	Dec 2019	2.193	Dec 2020	-		2.193	Continuing	Continuing	Continuing
Software Development	Various	Various : Various	67.520	0.495	Dec 2018	0.475	Dec 2019	0.680	Dec 2020	-		0.680	Continuing	Continuing	Continuing
Software Development	C/CPFF	BAH : San Diego, CA	8.527	2.609	Jan 2019	2.506	Jan 2020	1.517	Jan 2021	-		1.517	Continuing	Continuing	Continuing
Software Development	FFRDC	GTRI : Atlanta, GA	16.694	1.897	Jan 2019	2.917	Jan 2020	1.043	Jan 2021	-		1.043	Continuing	Continuing	Continuing
Software Development	WR	NSMA : San Diego, CA	3.744	1.519	Oct 2018	1.459	Oct 2019	0.937	Oct 2020	-		0.937	Continuing	Continuing	Continuing
Software Development	WR	NRL : Washington DC	3.058	0.841	Oct 2018	0.808	Oct 2019	1.439	Oct 2020	-		1.439	Continuing	Continuing	Continuing
		Subtotal	389.508	36.546		35.355		31.403		-		31.403	Continuing	Continuing	N/A

Exhibit R-3, RDT&E Project Cost Analysis: PB 2021 Navy		Date: February 2020
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 0734 / *Communications Security R&D*

Support ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2019 Cost	FY 2019 Award Date	FY 2020 Cost	FY 2020 Award Date	FY 2021 Base Cost	FY 2021 Base Award Date	FY 2021 OCO Cost	FY 2021 OCO Award Date	FY 2021 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Architecture	WR	Various : Various	5.911	0.231	Oct 2018	0.222	Oct 2019	0.138	Oct 2020	-		0.138	Continuing	Continuing	Continuing
Architecture	WR	NIWC ATLANTIC : Charleston, SC	2.502	0.441	Oct 2018	0.424	Oct 2019	0.404	Oct 2020	-		0.404	Continuing	Continuing	Continuing
Architecture	WR	NIWC PACIFIC : San Diego, CA	0.000	0.000		0.000		0.450	Oct 2020	-		0.450	Continuing	Continuing	Continuing
Requirements Analysis	C/CPFF	BAH : San Diego, CA	6.263	0.387	Jan 2019	0.372	Jan 2020	0.968	Jan 2021	-		0.968	Continuing	Continuing	Continuing
Studies & Design	WR	Various : Various	6.670	0.387	Oct 2018	0.372	Oct 2019	0.339	Oct 2020	-		0.339	Continuing	Continuing	Continuing
		Subtotal	21.346	1.446		1.390		2.299		-		2.299	Continuing	Continuing	N/A

Test and Evaluation ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2019 Cost	FY 2019 Award Date	FY 2020 Cost	FY 2020 Award Date	FY 2021 Base Cost	FY 2021 Base Award Date	FY 2021 OCO Cost	FY 2021 OCO Award Date	FY 2021 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
System DT&E	WR	NIWC PACIFIC : San Diego, CA	38.298	0.310	Oct 2018	0.298	Oct 2019	0.788	Oct 2020	-		0.788	Continuing	Continuing	Continuing
System DT&E	WR	COTF : Norfolk, VA	2.036	0.679	Dec 2018	0.652	Dec 2019	0.000		-		0.000	0.000	3.367	-
System DT&E	C/CPFF	BAH : San Diego, CA	2.218	0.799	Jan 2019	0.767	Jan 2020	1.000	Jan 2021	-		1.000	Continuing	Continuing	Continuing
System DT&E	WR	NIWC ATLANTIC : Charleston, SC	0.000	0.000		0.000		0.234	Oct 2020	-		0.234	0.000	0.234	-
		Subtotal	42.552	1.788		1.717		2.022		-		2.022	Continuing	Continuing	N/A

Management Services ($ in Millions)

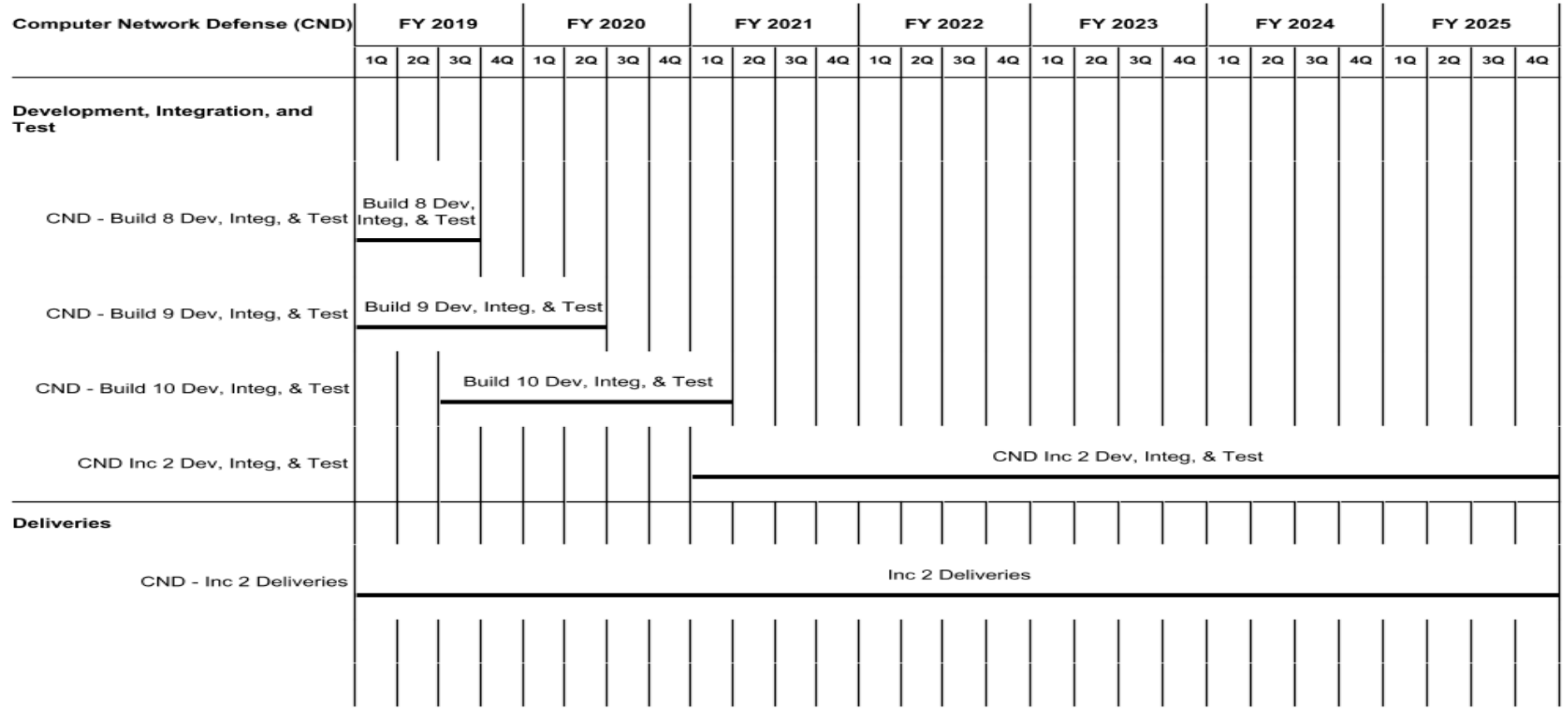
Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2019 Cost	FY 2019 Award Date	FY 2020 Cost	FY 2020 Award Date	FY 2021 Base Cost	FY 2021 Base Award Date	FY 2021 OCO Cost	FY 2021 OCO Award Date	FY 2021 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Program Management	C/CPFF	BAH : San Diego, CA	30.784	1.303	Jan 2019	1.251	Jan 2020	1.200	Jan 2021	-		1.200	Continuing	Continuing	Continuing
		Subtotal	30.784	1.303		1.251		1.200		-		1.200	Continuing	Continuing	N/A

Exhibit R-3, RDT&E Project Cost Analysis: PB 2021 Navy			Date: February 2020
Appropriation/Budget Activity 1319 / 7	R-1 Program Element (Number/Name) PE 0303140N / *Information Sys Security Program*	Project (Number/Name) 0734 / *Communications Security R&D*	

	Prior Years	FY 2019		FY 2020		FY 2021 Base		FY 2021 OCO		FY 2021 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	484.190	41.083		39.713		36.924		-		36.924	Continuing	Continuing	N/A

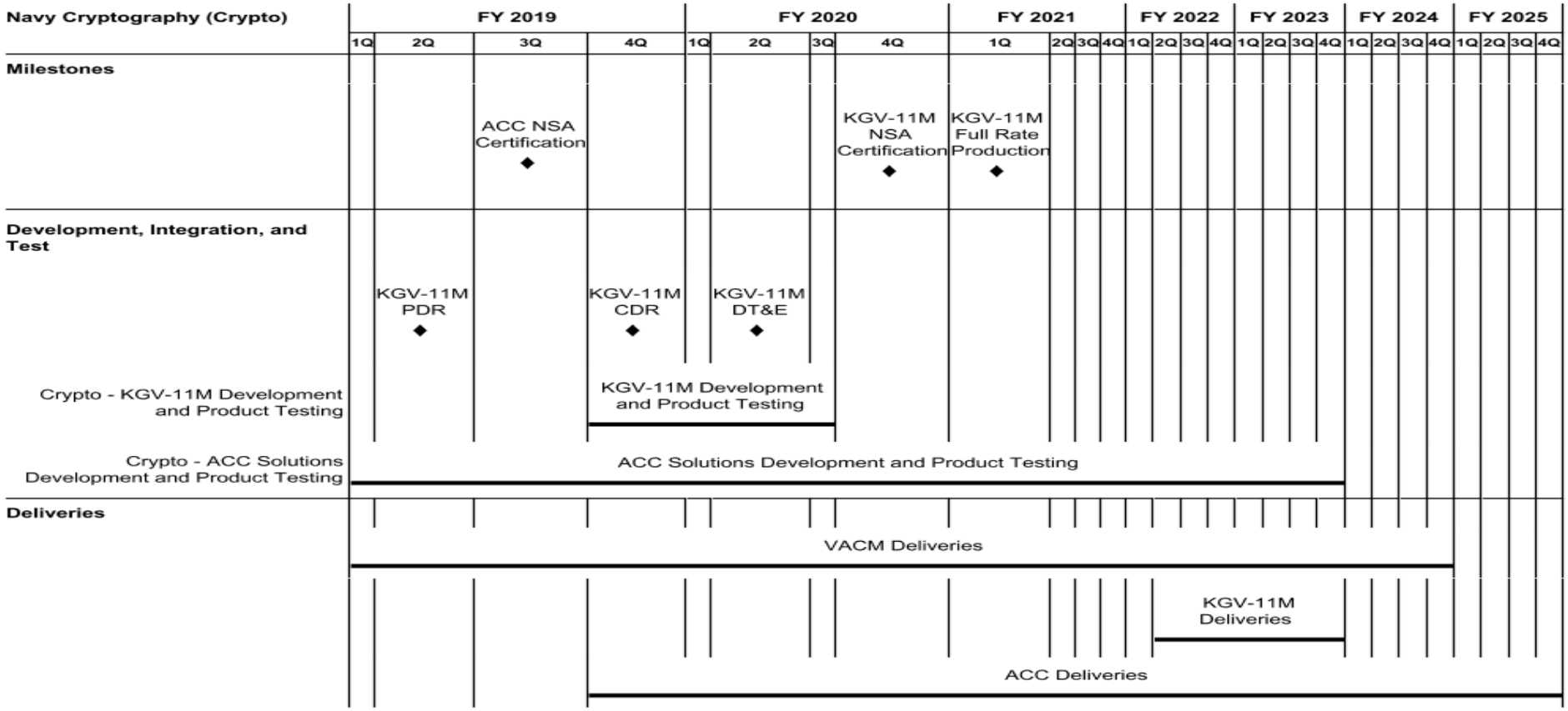
Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2021 Navy		Date: February 2020
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 0734 / *Communications Security R&D*



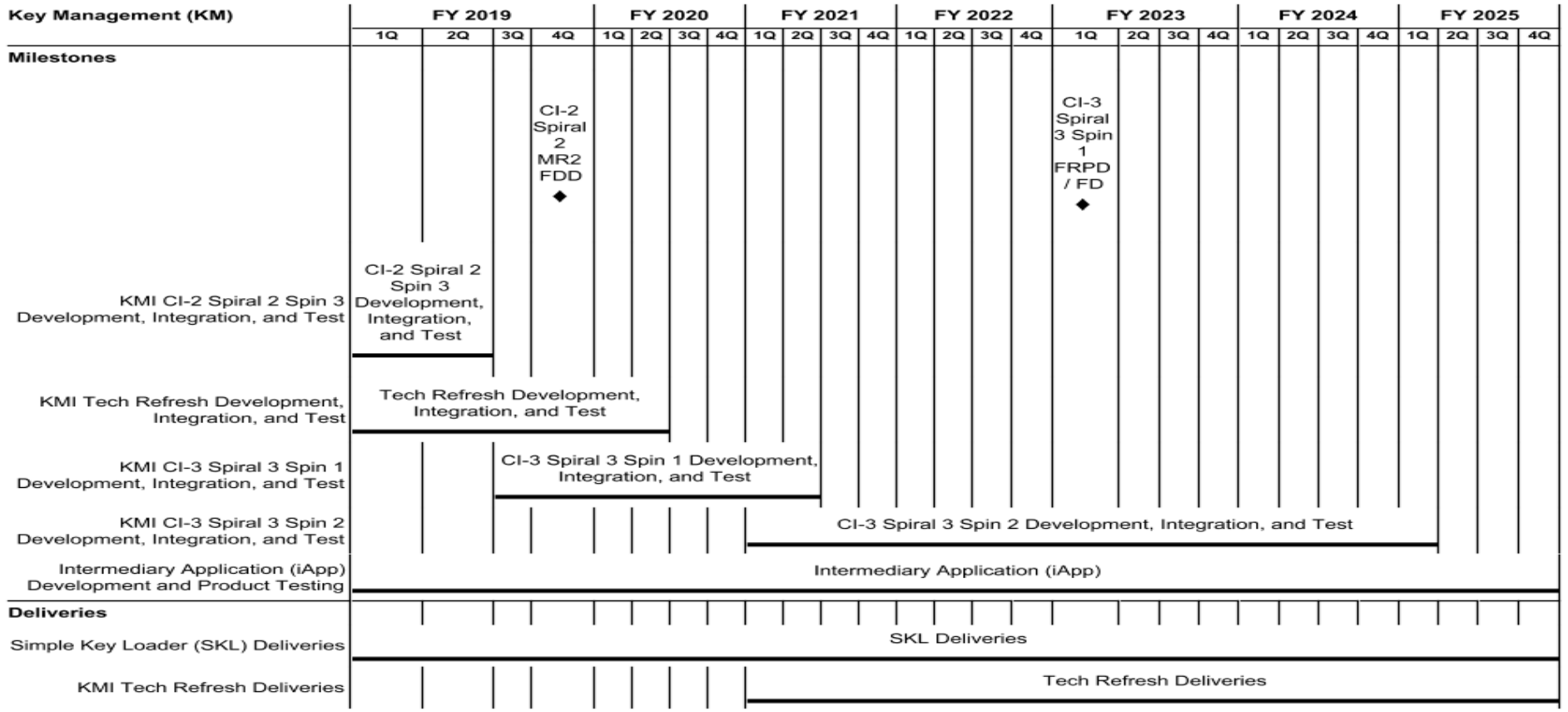
2021PB - 0303140N - 0734

Exhibit R-4, RDT&E Schedule Profile: PB 2021 Navy		Date: February 2020
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 0734 / *Communications Security R&D*



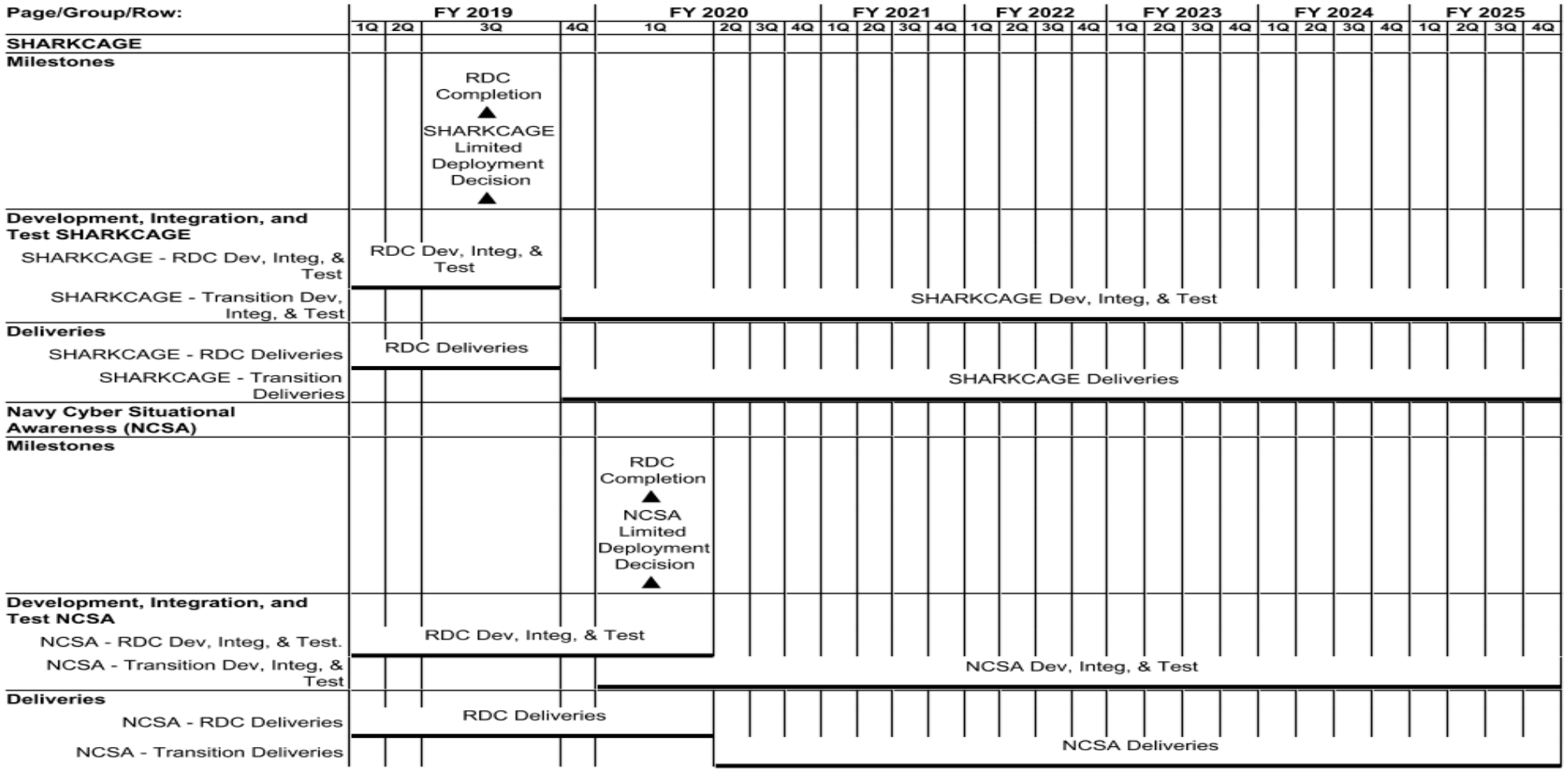
2021PB - 0303140N - 0734

Exhibit R-4, RDT&E Schedule Profile: PB 2021 Navy		Date: February 2020
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 0734 / *Communications Security R&D*



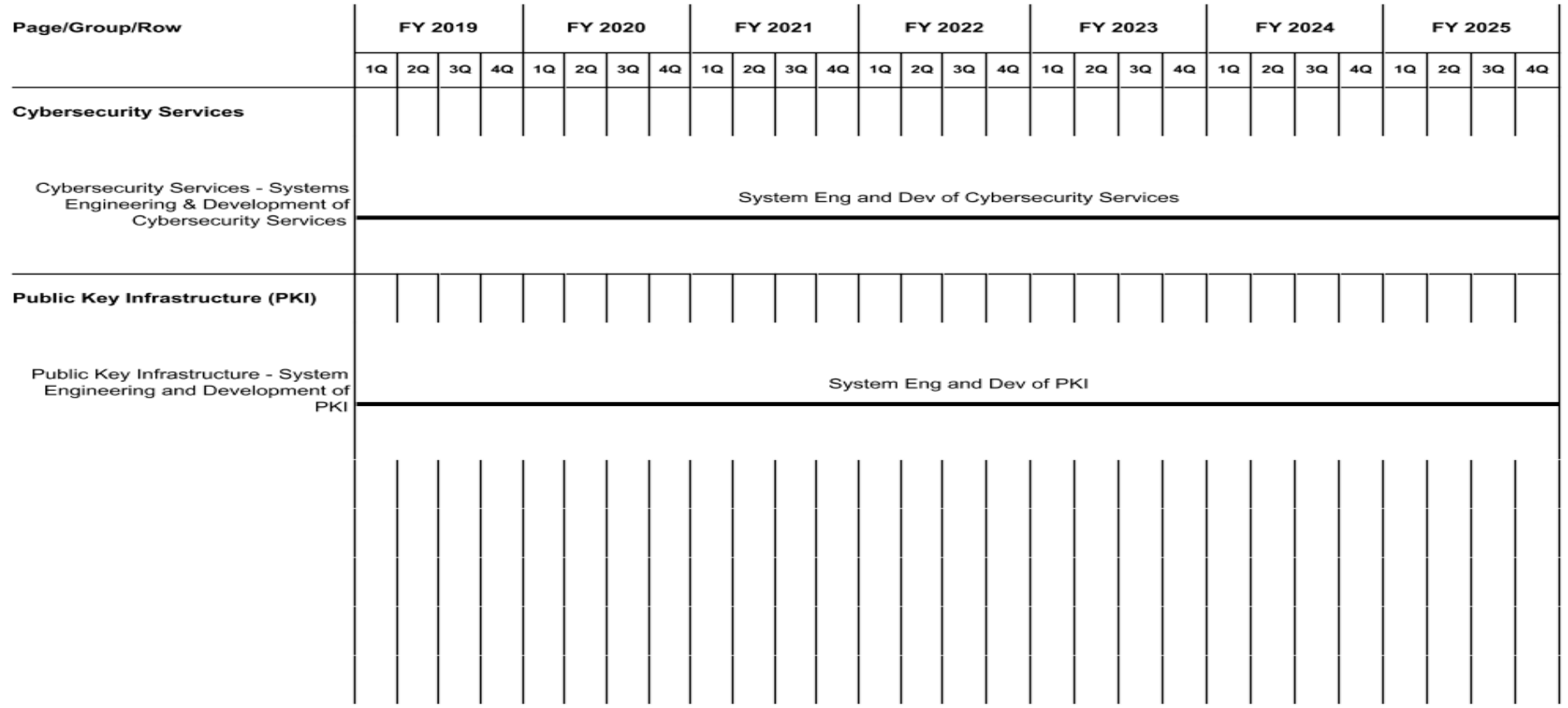
2021PB - 0303140N - 0734

Exhibit R-4, RDT&E Schedule Profile: PB 2021 Navy		Date: February 2020
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 0734 / *Communications Security R&D*



2021PB - 0303140N - 0734

Exhibit R-4, RDT&E Schedule Profile: PB 2021 Navy		Date: February 2020
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 0734 / *Communications Security R&D*



2021PB - 0303140N - 0734

Exhibit R-4A, RDT&E Schedule Details: PB 2021 Navy		Date: February 2020
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 0734 / *Communications Security R&D*

Schedule Details

	Start		End	
Events by Sub Project	**Quarter**	**Year**	**Quarter**	**Year**
Computer Network Defense (CND)				
Development, Integration, and Test: CND - Build 8 Dev, Integ, & Test:	1	2019	3	2019
Development, Integration, and Test: CND - Build 9 Dev, Integ, & Test:	1	2019	2	2020
Development, Integration, and Test: CND - Build 10 Dev, Integ, & Test:	3	2019	1	2021
Development, Integration, and Test: CND Inc 2 Dev, Integ, & Test:	1	2021	4	2025
Deliveries: CND - Inc 2 Deliveries:	1	2019	4	2025
Navy Cryptography (Crypto)				
Milestones: Crypto - KGV-11M NSA Certification	4	2020	4	2020
Milestones: Crypto - KGV-11M Full Rate Production	1	2021	1	2021
Milestones: Crypto - ACC NSA Certification	3	2019	3	2019
Development, Integration, and Test: Crypto - KGV-11M PDR	2	2019	2	2019
Development, Integration, and Test: Crypto - KGV-11M CDR	4	2019	4	2019
Development, Integration, and Test: Crypto - KGV-11M DT&E	2	2020	2	2020
Development, Integration, and Test: Crypto - KGV-11M Development and Product Testing:	4	2019	3	2020
Development, Integration, and Test: Crypto - ACC Solutions Development and Product Testing:	1	2019	4	2023
Deliveries: Crypto - VACM Deliveries	1	2019	4	2024
Deliveries: Crypto - KGV-11M Deliveries	2	2022	4	2023
Deliveries: Crypto - ACC Deliveries	4	2019	4	2025
Key Management (KM)				
Milestones: KMI CI-2 Spiral 2 MR2 Full Deployment Decision (FDD)	4	2019	4	2019
Milestones: KMI CI-3 Spiral 3 Spin 1 FRP Decision / FD	1	2023	1	2023

Exhibit R-4A, RDT&E Schedule Details: PB 2021 Navy		Date: February 2020
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 0734 / *Communications Security R&D*

	Start		End	
Events by Sub Project	**Quarter**	**Year**	**Quarter**	**Year**
Milestones: KMI CI-2 Spiral 2 Spin 3 Development, Integration, and Test:	1	2019	2	2019
Milestones: KMI Tech Refresh Development, Integration, and Test:	1	2019	2	2020
Milestones: KMI CI-3 Spiral 3 Spin 1 Development, Integration, and Test:	3	2019	2	2021
Milestones: KMI CI-3 Spiral 3 Spin 2 Development, Integration, and Test:	1	2021	1	2025
Milestones: Intermediary Application (iApp) Development and Product Testing:	1	2019	4	2025
Deliveries: Simple Key Loader (SKL) Deliveries:	1	2019	4	2025
Deliveries: KMI Tech Refresh Deliveries:	1	2021	4	2025
Page/Group/Row:				
Milestones: SHARKCAGE - RDC Completion	3	2019	3	2019
Milestones: SHARKCAGE - SHARKCAGE Transition Limited Deployment Decision	3	2019	3	2019
Development, Integration, and Test SHARKCAGE: SHARKCAGE - RDC Dev, Integ, & Test:	1	2019	3	2019
Development, Integration, and Test SHARKCAGE: SHARKCAGE - Transition Dev, Integ, & Test:	4	2019	4	2025
Deliveries: SHARKCAGE - RDC Deliveries:	1	2019	3	2019
Deliveries: SHARKCAGE - Transition Deliveries:	4	2019	4	2025
Milestones: NCSA - RDC Completion	1	2020	1	2020
Milestones: NCSA - NCSA Transition Limited Deployment Decision	1	2020	1	2020
Development, Integration, and Test NCSA: NCSA - RDC Dev, Integ, & Test.:	1	2019	1	2020
Development, Integration, and Test NCSA: NCSA - Transition Dev, Integ, & Test:	1	2020	4	2025
Deliveries: NCSA - RDC Deliveries:	1	2019	1	2020
Deliveries: NCSA - Transition Deliveries:	2	2020	4	2025
Page/Group/Row				
Cybersecurity Services: Cybersecurity Services - Systems Engineering & Development of Cybersecurity Services:	1	2019	4	2025

Exhibit R-4A, RDT&E Schedule Details: PB 2021 Navy		Date: February 2020
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 0734 / *Communications Security R&D*

	Start		End	
Events by Sub Project	**Quarter**	**Year**	**Quarter**	**Year**
Public Key Infrastructure (PKI): Public Key Infrastructure - System Engineering and Development of PKI:	1	2019	4	2025

Exhibit R-2A, RDT&E Project Justification: PB 2021 Navy			Date: February 2020
Appropriation/Budget Activity 1319 / 7	R-1 Program Element (Number/Name) PE 0303140N / *Information Sys Security Program*	Project (Number/Name) 3230 / *Information Assurance*	

COST ($ in Millions)	Prior Years	FY 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total	FY 2022	FY 2023	FY 2024	FY 2025	Cost To Complete	Total Cost
3230: *Information Assurance*	20.425	2.265	2.140	2.170	-	2.170	2.216	2.256	2.301	2.347	Continuing	Continuing
Quantity of RDT&E Articles		-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

The goal of the Information Systems Security Program (ISSP) is to ensure the continued protection of Navy and joint information and information systems from hostile exploitation and attack. The ISSP activities address the triad of Defense Information Operations: protection, detection, and reaction. Evolving attack sensing (detection), warning, and response (reaction) responsibilities extend far beyond the traditional ISSP role in the protection of Information Systems, including weapons systems. Focused on the highly mobile forward deployed subscriber, the Navy's adoption of Network-Centric Warfare (NCW) places demands upon the ISSP, as the number of users expands significantly and the criticality of their use escalates. Today, the ISSP protects an expanding core of services critical to the effective performance of the Navy's mission, as well as developing information assurance technology and systems that are resilient and survivable in the face of adversarial attacks. Features that are critical in supporting the Navy's concept of Distributed Maritime Operations (DMO).

The rapid rate of change in the underlying commercial and government information infrastructures makes the provision of security an increasingly complex and dynamic problem. IA technology mix and deployment strategies must evolve quickly to meet rapidly evolving threats and vulnerabilities. No longer can information security be divorced from the information infrastructure. The ISSP enables the Navy's war fighter to trust in the availability, integrity, authentication, privacy, and non-repudiation of information.

This project includes funds for advanced technology development, test and evaluation of naval information systems security based on leading edge technologies that will improve information assurance (e.g., situational awareness and information infrastructure protection) across all command echelons to tactical units afloat and war fighters ashore. This effort will provide the research to develop a secure seamless interoperable, common operational environment of networked information systems in the battle space and for monitoring and protecting the information infrastructure from malicious activities. This effort will provide naval forces a secure capability and basis in its achievement of protection from unauthorized access and misuse, and optimized IA resource allocations in the information battle space. This program will also develop core technology to: (1) improve network infrastructure resistance and resiliency to attacks; (2) enable the rapid development and certification of security-aware applications and information technologies in accordance with the common criteria for IA and IA-enabled information technology products by the National Security Telecommunications and Information Systems Security Committee; and (3) measure the effectiveness and efficiency of IA defensive capabilities under naval environments.

The program will develop common architectural frameworks that facilitate integration of network security capabilities, enable effective seamless interoperation, and contribute to a common consistent picture of the networked environment with respect to information assurance and security. This effort will address the need for a common operational picture for IA, as well as assessment of security technology critical to the success of the mission. This effort will also initiate requirements definition for situational awareness capabilities to support computer network defense in a highly-distributed, homogeneous, and heterogeneous networks including mobile and embedded networked devices. This effort also includes the architectural definition of situational awareness and visualization capabilities to support active computer network defense and support underlying data mining and correlation tools. This includes addressing the capability to remotely manage and securely control the

Exhibit R-2A, RDT&E Project Justification: PB 2021 Navy		Date: February 2020
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 3230 / *Information Assurance*

configurations of network security components to implement changes in real time or near real time. This program will also initiate requirements definition for secure coalition data exchange and interoperation among security levels and classifications, and ensure approaches address various security level technologies as well as emerging architectural methods of providing interoperability across different security levels. IA will examine multi-level aware applications and technologies including databases, web browsers, routers/switches, etc. Efforts will also initiate infrastructure protection efforts as the Navy develops network centric architectures and warfare concepts, ensuring an evolutionary development of security architectures and products for IA that addresses Navy infrastructure requirements. IA will ensure the architectures evolve to provide proper protection as technology, Department of Defense (DoD) missions, and threats continuously evolve. IA includes defensive protections as well as intrusion monitoring (sensors), warning mechanisms, and response capabilities in the architecture. Ensure the unique security and performance requirements of tactical systems, including those operating various security levels are addressed. Also, the program will initiate the efforts to conceptualize new network centric warfare technology to protect our assets, such as secure network gateways, routers, components and tools that improve the survivability of Navy networks. Additionally, IA will provide systems security engineering, certification and accreditation support for high-confidence naval information systems and ensure certification and accreditation approaches are consistent with Navy and DoD requirements.

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total
Title: Information Assurance (IA)	2.265	2.140	2.170	0.000	2.170
Articles:	-	-	-	-	-
FY 2020 Plans: Complete the development of a new techniques/technology for discovering adversarial presence in Navy/ DoD networks, especially for APT within the network infrastructure and components/workstations. Efforts will focus on detection, isolation and remediation while maintaining continuity of operations and access to critical data. Complete the development of new technology to support asset criticality and management to improve effectiveness of cyber defenses in support of mission execution, focusing on threats and attack propagation through the network. Continue systems security engineering, certification and accreditation support for high-confidence, high criticality naval information systems and ensure certification and accreditation approaches are consistent with Navy and DoD requirements. Continue the development of a new generation of cross-domain technology that focuses on critical infrastructure protection while protecting against sophisticated nation state attacks and exfiltration, while supporting new data models and formats for emerging Navy networks. Continue the development of intelligent security components and infrastructure capable of protecting the DON's critical cyber assets through intelligent, autonomous self-diagnostics, automated damage assessment, and self-healing capabilities. Continue the development of a framework to systematically identify optimal and pertinent features of cyber behavior data in order to detect anomalies. Anomalies stemming from malicious cyber activity (e.g., intrusions, denial of service, malware) will be identified, as well as the development of metrics indicating the health and security posture of the cyber resources. Continue the development of algorithms that automatically identify the feature space and select the optimal feature set from the given cyber data, the network traffic, and the interconnectivity of the cyber resources. Initiate the development of tools to automatically analyze and					

Exhibit R-2A, RDT&E Project Justification: PB 2021 Navy		Date: February 2020
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 3230 / *Information Assurance*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total
reverse engineer malware of unknown provenance at scale. Includes rapid prototyping and fielding of novel digital content inspection mechanisms that identify indicators of compromise and generate tailored defensive countermeasures to emerging cyber threats. ***FY 2021 Base Plans:*** - Complete the development of a new generation of cross-domain technology that focuses on critical infrastructure protection while protecting against sophisticated nation state attacks and exfiltration, while supporting new data models and formats for emerging Navy networks. - Ensure technology meets low-latency requirements of interconnecting naval systems. - Complete the development of a framework to systematically identify optimal and pertinent features of cyber behavior data in order to detect anomalies. Anomalies stemming from malicious cyber activity (e.g., intrusions, denial of service, malware) will be identified, as well as the development of metrics indicating the health and security posture of the cyber resources. - Complete the development of algorithms that automatically identify the feature space and select the optimal feature set from the given cyber data, the network traffic, and the interconnectivity of the cyber resources. - Continue the development of intelligent security components and infrastructure capable of protecting the DON's critical cyber assets through intelligent, autonomous self-diagnostics, automated damage assessment, and self-healing capabilities. - Continue systems security engineering, certification and accreditation support for high-confidence, high criticality naval information systems and ensure certification and accreditation approaches are consistent with Navy and DoD requirements. - Continue the development of tools to automatically analyze and reverse engineer malware of unknown provenance at scale. This includes rapid prototyping and fielding of novel digital content inspection mechanisms that identify indicators of compromise and generate tailored defensive countermeasures to emerging cyber threats. - Initiate the development of new cyber tools/technology to provide dynamic maneuvering/moving target defense of critical naval assets to reduce the attack surface and obviate vulnerabilities prior to exploitation. This includes addressing protocols, input/output resources and stacks, and system software; with emphasis on advanced persistent threats (APTs). ***FY 2021 OCO Plans:*** N/A ***FY 2020 to FY 2021 Increase/Decrease Statement:***					

Exhibit R-2A, RDT&E Project Justification: PB 2021 Navy		Date: February 2020
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 3230 / *Information Assurance*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total
No significant changes from FY20 to FY21; no programmatic impact.					
Accomplishments/Planned Programs Subtotals	2.265	2.140	2.170	0.000	2.170

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A

Exhibit R-3, RDT&E Project Cost Analysis: PB 2021 Navy			Date: February 2020
Appropriation/Budget Activity 1319 / 7	R-1 Program Element (Number/Name) PE 0303140N / *Information Sys Security Program*	Project (Number/Name) 3230 / *Information Assurance*	

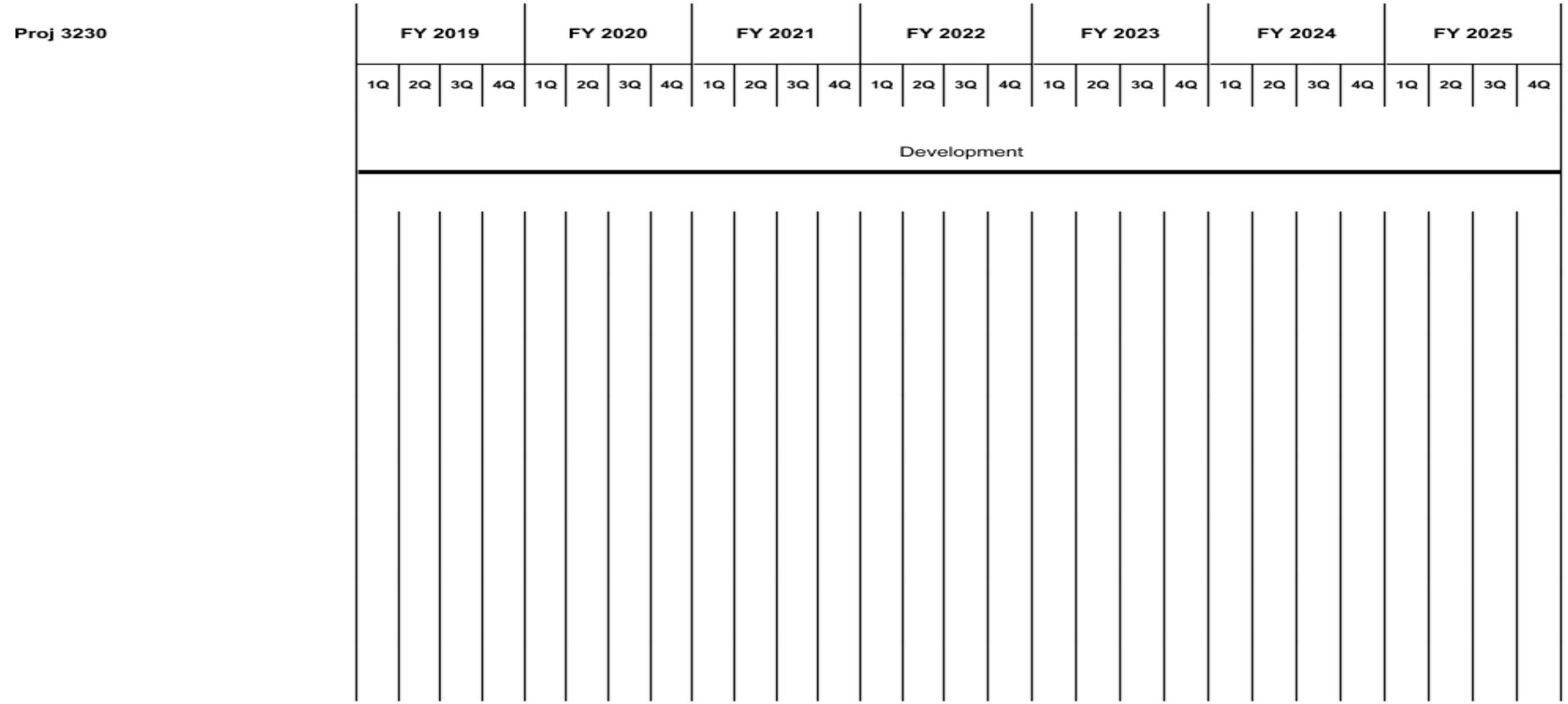
Support ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2019 Cost	FY 2019 Award Date	FY 2020 Cost	FY 2020 Award Date	FY 2021 Base Cost	FY 2021 Base Award Date	FY 2021 OCO Cost	FY 2021 OCO Award Date	FY 2021 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Development Support	Various	NRL : Washington, DC	20.425	2.265	Nov 2018	2.140	Nov 2019	2.170	Nov 2020	-		2.170	Continuing	Continuing	Continuing
		Subtotal	20.425	2.265		2.140		2.170		-		2.170	Continuing	Continuing	N/A

	Prior Years	FY 2019		FY 2020		FY 2021 Base		FY 2021 OCO		FY 2021 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	20.425	2.265		2.140		2.170		-		2.170	Continuing	Continuing	N/A

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2021 Navy		Date: February 2020
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 3230 / *Information Assurance*



2021OSD - 0303140N - 3230

Exhibit R-4A, RDT&E Schedule Details: PB 2021 Navy		Date: February 2020
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 3230 / *Information Assurance*

Schedule Details

	Start		End	
Events by Sub Project	**Quarter**	**Year**	**Quarter**	**Year**
Proj 3230				
Development	1	2019	4	2025

Exhibit R-2A, RDT&E Project Justification: PB 2021 Navy			Date: February 2020
Appropriation/Budget Activity 1319 / 7	R-1 Program Element (Number/Name) PE 0303140N / *Information Sys Security Program*	Project (Number/Name) 9999 / *Congressional Adds*	

COST ($ in Millions)	Prior Years	FY 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total	FY 2022	FY 2023	FY 2024	FY 2025	Cost To Complete	Total Cost
9999: *Congressional Adds*	0.000	0.000	3.000	0.000	-	0.000	0.000	0.000	0.000	0.000	0.000	3.000
Quantity of RDT&E Articles		-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

The goal of the Information Systems Security Program (ISSP) is to ensure the continued protection of Navy and joint information and information systems from hostile exploitation and attack. The ISSP activities address the triad of Defense Information Operations: protection, detection, and reaction. Evolving attack sensing (detection), warning, and response (reaction) responsibilities extend far beyond the traditional ISSP role in the protection of Information Systems, including weapons systems. Focused on the highly mobile forward deployed subscriber, the Navy's adoption of Network-Centric Warfare (NCW) places demands upon the ISSP, as the number of users expands significantly and the criticality of their use escalates. Today, the ISSP protects an expanding core of services critical to the effective performance of the Navy's mission, as well as developing information assurance technology and systems that are resilient and survivable in the face of adversarial attacks. Features that are critical in supporting the Navy's concept of Distributed Maritime Operations (DMO).

The rapid rate of change in the underlying commercial and government information infrastructures makes the provision of security an increasingly complex and dynamic problem. IA technology mix and deployment strategies must evolve quickly to meet rapidly evolving threats and vulnerabilities. No longer can information security be divorced from the information infrastructure. The ISSP enables the Navy's war fighter to trust in the availability, integrity, authentication, privacy, and non-repudiation of information.

This project includes funds for advanced technology development, test and evaluation of naval information systems security based on leading edge technologies that will improve information assurance (e.g., situational awareness and information infrastructure protection) across all command echelons to tactical units afloat and war fighters ashore. This effort will provide the research to develop a secure seamless interoperable, common operational environment of networked information systems in the battle space and for monitoring and protecting the information infrastructure from malicious activities. This effort will provide naval forces a secure capability and basis in its achievement of protection from unauthorized access and misuse, and optimized IA resource allocations in the information battle space. This program will also develop core technology to: (1) improve network infrastructure resistance and resiliency to attacks; (2) enable the rapid development and certification of security-aware applications and information technologies in accordance with the common criteria for IA and IA-enabled information technology products by the National Security Telecommunications and Information Systems Security Committee; and (3) measure the effectiveness and efficiency of IA defensive capabilities under naval environments.

The program will develop common architectural frameworks that facilitate integration of network security capabilities, enable effective seamless interoperation, and contribute to a common consistent picture of the networked environment with respect to information assurance and security. This effort will address the need for a common operational picture for IA, as well as assessment of security technology critical to the success of the mission. This effort will also initiate requirements definition for situational awareness capabilities to support computer network defense in a highly-distributed, homogeneous, and heterogeneous networks including mobile and embedded networked devices. This effort also includes the architectural definition of situational awareness and visualization capabilities to support active computer network defense and support underlying data mining and correlation tools. This includes addressing the capability to remotely manage and securely control the

Exhibit R-2A, RDT&E Project Justification: PB 2021 Navy		Date: February 2020
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 9999 / *Congressional Adds*

configurations of network security components to implement changes in real time or near real time. This program will also initiate requirements definition for secure coalition data exchange and interoperation among security levels and classifications, and ensure approaches address various security level technologies as well as emerging architectural methods of providing interoperability across different security levels. IA will examine multi-level aware applications and technologies including databases, web browsers, routers/switches, etc. Efforts will also initiate infrastructure protection efforts as the Navy develops network centric architectures and warfare concepts, ensuring an evolutionary development of security architectures and products for IA that addresses Navy infrastructure requirements. IA will ensure the architectures evolve to provide proper protection as technology, Department of Defense (DoD) missions, and threats continuously evolve. IA includes defensive protections as well as intrusion monitoring (sensors), warning mechanisms, and response capabilities in the architecture. Ensure the unique security and performance requirements of tactical systems, including those operating various security levels are addressed. Also, the program will initiate the efforts to conceptualize new network centric warfare technology to protect our assets, such as secure network gateways, routers, components and tools that improve the survivability of Navy networks. Additionally, IA will provide systems security engineering, certification and accreditation support for high-confidence naval information systems and ensure certification and accreditation approaches are consistent with Navy and DoD requirements.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2019	FY 2020
Congressional Add: High assurance infrastructure in defense systems	0.000	3.000
FY 2019 Accomplishments: N/A		
FY 2020 Plans: - Conduct developmental and engineering efforts to of cybersecurity tools, cryptographic acceleration and key management to protect Navy networks and infrastructure of defense systems.		
Congressional Adds Subtotals	0.000	3.000

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A

Exhibit R-3, RDT&E Project Cost Analysis: PB 2021 Navy		Date: February 2020
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 9999 / *Congressional Adds*

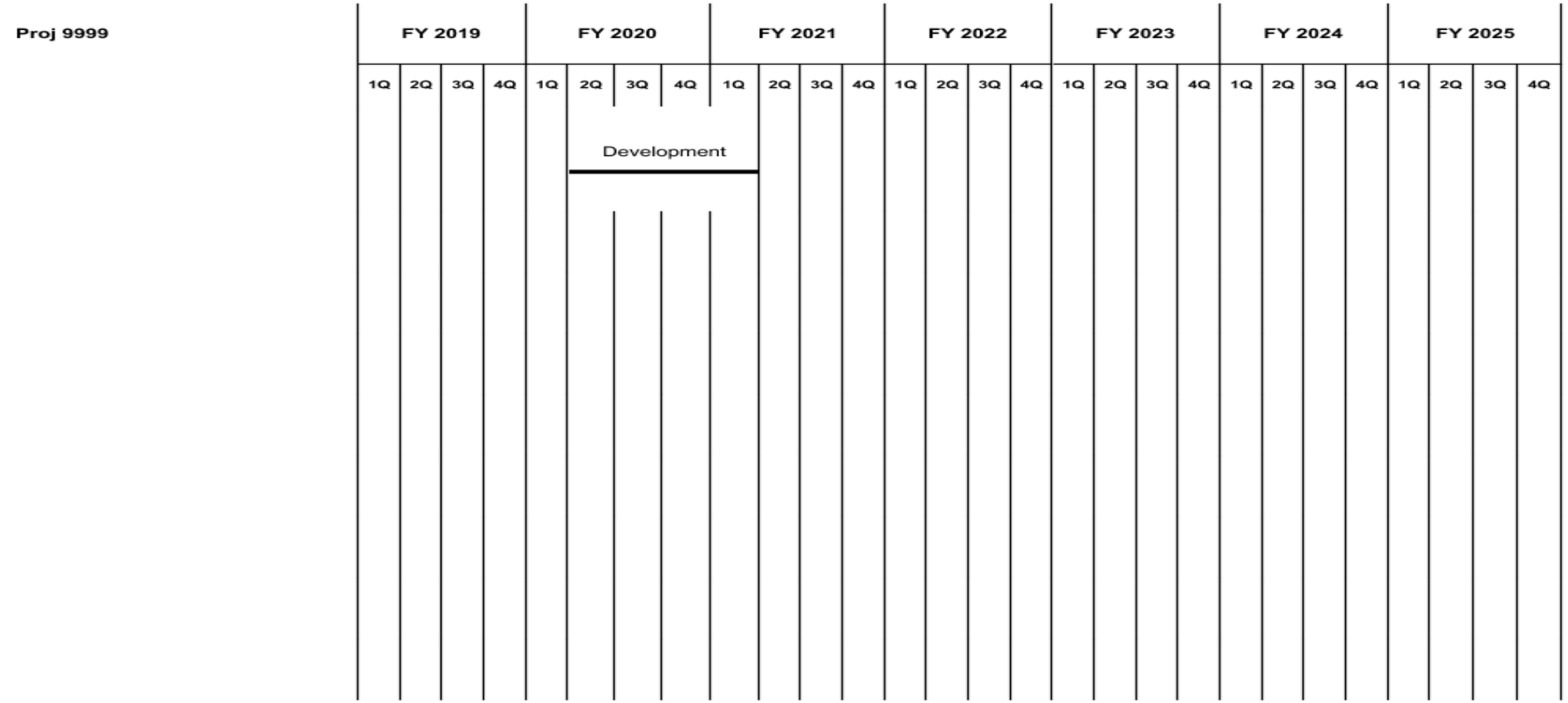
Product Development ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2019 Cost	FY 2019 Award Date	FY 2020 Cost	FY 2020 Award Date	FY 2021 Base Cost	FY 2021 Base Award Date	FY 2021 OCO Cost	FY 2021 OCO Award Date	FY 2021 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Software Development	WR	NIWC ATLANTIC : Charleston, SC	0.000	0.000		3.000	Jan 2020	0.000		-		0.000	0.000	3.000	-
		Subtotal	0.000	0.000		3.000		0.000		-		0.000	0.000	3.000	N/A

	Prior Years	FY 2019		FY 2020		FY 2021 Base		FY 2021 OCO		FY 2021 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	0.000	0.000		3.000		0.000		-		0.000	0.000	3.000	N/A

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2021 Navy		Date: February 2020
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 9999 / *Congressional Adds*



2021PB - 0303140N - 9999

Exhibit R-4A, RDT&E Schedule Details: PB 2021 Navy		Date: February 2020
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 9999 / *Congressional Adds*

Schedule Details

	Start		End	
Events by Sub Project	**Quarter**	**Year**	**Quarter**	**Year**
Proj 9999				
Development	2	2020	1	2021